IN THE CLAIMS

Please amend Claim 24.

Claims 1-23 Cancelled

24. (Currently Amended) A method for caching secure content in a Secure Reverse Proxy ("SRP") in an secure network, comprising:

coupling at least one SRP among at least one web browser and at least one web server wherein the at least one SRP receives from the at least one web browser requests for establishing a first secure session;

establishing the first secure session using a first secure session protocol between the at least one SRP and the at least on web browser, wherein the web browser sends an encrypted request for content to the at least one SRP;

decrypting the encrypted request for content from the at least one web browser at the at least one SRP using the first secure session protocol, wherein the at least one SRP determines that the at least one SRP does not possess the requested content;

establishing a second secure session using a second secure session protocol between the at least one SRP and the at least one web server, wherein the second secure session is maintained;

encrypting the request for content from the at least one web browser using the second secure session protocol;

sending the encrypted request for content to the at least one web server using the second secure session;

receiving the content from the at least one web server at the least one SRP using the second secure session;

decrypting the content using the second secure session protocol;

encrypting said content using the first secure session protocol for sending, using the first session, to the at least one web browser in response to the encrypted request for content;

encrypting the requested content using a third secure session protocol; for storing the encrypted requested content locally in a memory at the at least one SRP; and

retrieving the content from the memory at the at least one SRP upon subsequent requests for the content.

25. (Previously presented) The method of claim 24, wherein the third secure session protocol is known only to the at least one SRP.

26. (Original) The method of claim 24, wherein storing includes using non-volatile media.

27. (Original) The method of claim 24, wherein coupling includes establishing a dedicated secure line between the SRP and the web server.

28. (Original) The method of claim 24, wherein coupling includes collocating the web server and the SRP.

29. (Original) The method of claim 24, wherein content includes an HTTP page.

30. (Original) The method of claim 24, wherein the first secure session includes Transport Layer Security protocol.

31. (Original) The method of claim 24, wherein the second secure session includes Transport Layer Security protocol.

32. (Original) The method of claim 24, wherein the first secure session includes Secure Socket Layer protocol.

33. (Original) The method of claim 24, wherein the second secure session includes Secure Socket Layer protocol.

34. (Original) The method of claim 24, wherein the first secure session includes Internet Protocol Secure ("IPSec") techniques.

35. (Original) The method of claim 24, wherein the second secure session includes Internet Protocol Secure ("IPSec") techniques.

36. (Previously presented) The method of claim 29, further comprising, before storing the HTTP page, encrypting the HTTP page.

Claims 37-50 Cancelled

51. (Previously presented) A Secure Reverse Proxy ("SRP") appliance for caching secure content in a secure network, the SRP appliance comprising:

a processing mechanism;

an encryption and decryption mechanism; and

a tamper-resistant mechanism for storing one or more keys, wherein the one or more keys are known only to the SRP and are used for encrypting the content before storing the content in a secure local cache for future requests for the content.

52. (Previously presented) The SRP appliance of Claim 51, wherein the tamper-resistant mechanism includes a tamper-resistant non-volatile card.

53. (Previously presented) The SRP appliance of Claim 51, wherein the local cache includes non-volatile memory.

54. (Previously presented) The SRP appliance of Claim 51, wherein the SRP appliance is configured for using a secure protocol.

55. (Previously presented) The SRP appliance of Claim 51, wherein the SRP appliance is configured for using a Secure Socket Layer protocol.

56. (Previously presented) The SRP appliance of Claim 51, wherein the SRP appliance is configured for using Internet Protocol Secure ("IPSec") techniques.

57. (Previously presented) The SRP appliance of Claim 51, wherein the SRP appliance is configured for using a Transport Layer Security Protocol.

58. (Previously presented) The SRP appliance of Claim 51, wherein the SRP appliance is coupled among at least one web server and at least one web browser, wherein the SRP appliance intercepts requests from the at least one web browser to establish a secure network communication session with the at least one web server.